Security Education and Risk - Protecting Your Business

Mark Knowles
General Manager Security Assurance
19 October 2022 - CybersecCon 2022

External(np)

What to Expect from this Session

I plan to make this so simple, I want you to be able to use something, a Gem to help you to protect your Business

“I’ve heard this before!” “Heard it ages ago and it hasn't happened to me” “I know it could happen, but I am way to busy, or I can't get the support, the money I need”

An idea or a strategy that will help protect you, your customers, your employees no matter what your role is.

Xero - What we are doing, why I think we have that “Gem”

Security Education and Risk - Protecting Your Business

Are we acting fast enough?

92% of Attacks are Phishing

More and more sophisticated

Regular attacks

Look very very real

Cyber criminals sending millions of these

Designed to catch just one of you

Ransomware - 10%

The Cyber criminal taking full control of all your Data

Multiple goals for the criminals

- Financial
- Personal Information
- Frustration

Impact of the Pandemic, War in the Ukraine

Increasing economic challenges/ pressures

Cyber criminals attack when people are the most vulnerable

Family members impacted causing unseen mental health pressures

External(np)

What can you do to stay safe?

External(np)

What can you do to stay safe?

People

Process

Technology

Be Prepared

Practice many different types of challenges

- Invest some time every month to work with your teams to see how you would react if a cyber event was to happen

Phishing Simulations

Test yourself and your teams on a regular basis with Phishing simulations

- There are some great Phishing Simulation services available
- Consider just practising on some emails you have in your inbox with your team

Business Continuity Planning/ Health Practices

Do you have a documented BCP? When did you last check?

- Is your Critical data backed up
- Is Multi Factor Authentication in place
- Do you use a Password Manager?

Identifying Risks

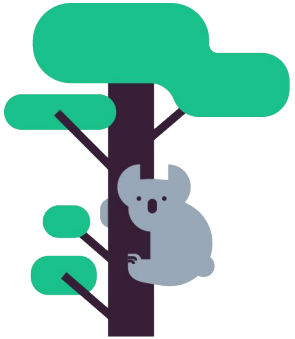
Share Vulnerability examples

Use Real Case Studies with your teams

We are all at risk no matter what our role, our experience .....

30 Seconds could save you from a lot of pain

Record the Risks - What makes you Vulnerable?



Use your Practice, record the learning, consider reasons that could make you vulnerable?

How did people react in the table to exercise?

- Was there a natural leader?
- What was missing?
- Would you panic if it was real?

What would make people click on Phishing emails?

- Discuss the things people clicked
- Who's had phishing emails at home?
- Why wouldn't we talk about them?

How is your team feeling?

- Anyone showing signs of stress or being under pressure
- Know your people

What's the thing that you just have to have that would make you act before thinking?

Security Education and Risk - Protecting Your Business

Risk Management

Act - At Xero we have a Process, a plan and agreed standards

Preparation will reduce your pain

Visibility of the Risk

Ensure that your Risks are clear

- Avoid abbreviations
- The title clearly states what the risk is

All parties impacted by the risk must know that it is there

- Get input from all parties on the treatment plan

Increased Visibility has helped us to reduce the risk

Ownership

The Risk Owner needs to be the Accountable Owner

There will be teams that are responsible for helping with controls and mitigations

Agree the consequences of agreed treatment plans not being met

- Does it matter?
- Reward success
- Help each other with prioritization

Consistency and Action

Measure all risks using the same Impact and Likelihood and therefore Consequence scale

The most critical risk will be agreed by all

Ensure Treatment plans are agreed within a month of identifying the risk

Some risks may be accepted, have review dates in place and stick to the dates

Security Education and Risk - Protecting Your Business
CybersecCon 2022

Security Risks are Increasing

How do you scale?

How do we get the best for our investment?

External(np)

Creating Security Champions across Xero

We have established a Programme of work to enable our team members to become a Security Champion

- **It is a part of their normal job, no matter where they work within Xero**

Celebrating a Culture that embraces and supports Security

At Xero we talk about security, we take it seriously, we are proud of the work we do to maintain and build and grow a strong security posture

Embracing Security early enables us to ensure we have more chance of reducing our risks as just something we all do.

Security Champions and Culture Model

Security Ambassador
Chief and EGM GM level to represent all business areas. They have a strong voice for security and a high level of influence to their parts of the business.

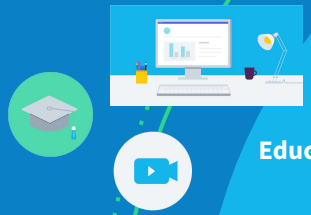
Security Champions
Being a conduit back and forward from their team to the Security Team and to better influence security in their team.

All Xeros
Everyone having a base understanding of security, better awareness and clear guidance on how to implement security in there job and role.

Security Teams
Supporting and enabling our champions and all Xeros.

ELEMENTS

The culture will come to life though using the five elements around the program



Education

Recognition

PEOPLE

The groups of people who play a role in Xero's security culture

Security Ambassador

Security Champions

All Xeros

Security Teams

Standards, policies & guidelines

#Ownership

Leadership

Keep it Simple
Just do it

Take Action - Practice/ Talk/ Learn

Solutions need People, Processes and Technology

Record the Risks and have a Plan

Build a Positive Security Culture

External(np)

Beautiful business